The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
7/26/2010

SUBJECT:
Vulnerability in Mozilla Firefox Could Allow Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Mozilla Firefox which could allow for remote code execution. Mozilla Firefox is a web browser used to access the Internet.

This vulnerability requires that a user visit or be redirected to a web page, or open a malicious file crafted to take advantage of this specific vulnerability. This vulnerability, if exploited, could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

Mozilla Firefox 3.6.7

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been identified for Mozilla Firefox which may allow for remote code execution. This vulnerability was caused by the Mozilla Firefox 3.6.7 release, which was recently pushed out to fix several previously disclosed vulnerabilities. According to Mozilla, the Firefox 3.6.7 release that was pushed out to resolve a plugin parameter array crash has unexpectedly resulted in a newly discovered crash which shows signs of memory corruption. Also, in certain instances the parameter array for a plugin instance could be freed too early resulting in a dangling pointer which could then be executed by the plugin.

In order for this vulnerability to be exploited a user would have to visit or be redirected to a web page, or open a malicious file specifically crafted to take advantage of this vulnerability. If successfully exploited this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

According to Mozilla, this vulnerability has been fixed in Firefox 3.6.8.

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade to Firefox 3.6.8 provided by Mozilla on vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to download or open files from un-trusted websites.

REFERENCES:

Mozilla Foundation Security:
http://www.mozilla.org/security/announce/2010/mfsa2010-48.html

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2755

Red Hat Bugzilla:
https://bugzilla.redhat.com/show_bug.cgi?id=617657

Security Focus:
http://www.securityfocus.com/bid/41933